

TRAITE DE COOPERATION EN MATIERE DE BREVETS

25 JUIN 2001

PCT

NOTIFICATION DE LA RECEPTION DE
L'EXEMPLAIRE ORIGINAL

(règle 24.2.a) du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

CORLU, Bernard
Bull CP8
PC62A24
68, route de Versailles
Boîte postale 45
F-78431 Louveciennes Cedex
FRANCE

Date d'expédition (jour/mois/année) 18 juin 2001 (18.06.01)	NOTIFICATION IMPORTANTE
Référence du dossier du déposant ou du mandataire PCT 3879/BC	Demande internationale no PCT/FR01/01359

Il est notifié au déposant que le Bureau international a reçu l'exemplaire original de la demande internationale précisée ci-après.

Nom(s) du ou des déposants et de l'Etat ou des Etats pour lesquels ils sont déposants:

BULL CP8 (pour tous les Etats désignés sauf US)

HAZARD, Michel (pour US seulement)

Date du dépôt international : 04 mai 2001 (04.05.01)
Date(s) de priorité revendiquée(s) : 09 mai 2000 (09.05.00)
Date de réception de l'exemplaire original
par le Bureau international : 05 juin 2001 (05.06.01)

Liste des offices désignés :

EP : AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR
National : AU, BR, CA, CN, JP, KR, NO, SG, US

ATTENTION

Le déposant doit soigneusement vérifier les indications figurant dans la présente notification. En cas de divergence entre ces indications et celles que contient la demande internationale, il doit aviser immédiatement le Bureau international.

En outre, l'attention du déposant est appelée sur les renseignements donnés dans l'annexe en ce qui concerne

- ☒ les délais dans lesquels doit être abordée la phase nationale
☒ la confirmation des désignations faites par mesure de précaution
☐ les exigences relatives aux documents de priorité.

Une copie de la présente notification est envoyée à l'office récepteur et à l'administration chargée de la recherche internationale.

Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse n° de télécopieur (41-22) 740.14.35	Fonctionnaire autorisé Philippe Bécamel n° de téléphone (41-22) 338.83.38
---	---

**RENSEIGNEMENTS CONCERNANT LES DELAIS DANS LESQUELS DOIT ETRE ABORDEE
LA PHASE NATIONALE**

Il est rappelé au déposant qu'il doit aborder la "phase nationale" auprès de chacun des offices désignés indiqués sur la notification de la réception de l'exemplaire original (formulaire PCT/IB/301) en payant les taxes nationales et en remettant les traductions, telles qu'elles sont prescrites par les législations nationales.

Le délai d'accomplissement de ces actes de procédure est de **20 MOIS** à compter de la date de priorité ou, pour les Etats désignés qui ont été élus par le déposant dans une demande d'examen préliminaire internationale ou dans une élection ultérieure, de **30 MOIS** à compter de la date de priorité, à condition que cette élection ait été effectuée avant l'expiration du 19^e mois à compter de la date de priorité. Certains offices désignés (ou élus) ont fixé des délais qui expirent au-delà de 20 ou 30 mois à compter de la date de priorité. D'autres offices accordent une prolongation des délais ou un délai de grâce, dans certains cas moyennant le paiement d'une taxe supplémentaire.

En plus de ces actes de procédure, le déposant devra dans certains cas satisfaire à d'autres exigences particulières applicables dans certains offices. **Il appartient au déposant** de veiller en temps voulu les conditions requises pour l'ouverture de la phase nationale. La majorité des offices désignés n'envoient pas de rappel à l'approche de la date limite pour aborder la phase nationale.

Des informations détaillées concernant les actes de procédure à accomplir pour aborder la phase nationale auprès de chaque office désigné, les délais applicables et la possibilité d'obtenir une prolongation des délais ou un délai de grâce et toutes autres conditions applicables figurent dans le volume II du Guide du déposant du PCT. Les exigences concernant le dépôt d'une demande d'examen préliminaire international sont exposées dans le chapitre IX du volume I du Guide du déposant du PCT.

GR et ES sont devenues liées par le chapitre II du PCT le 7 septembre 1996 et le 6 septembre 1997, respectivement, et peuvent donc être élues dans une demande d'examen préliminaire international ou dans une élection ultérieure présentée le 7 septembre 1996 (ou à une date postérieure) ou le 6 septembre 1997 (ou à une date postérieure), respectivement, quelle que soit la date de dépôt de la demande internationale (voir le second paragraphe, ci-dessus).

Veuillez noter que seul un déposant qui est ressortissant d'un Etat contractant du PCT lié par le chapitre II ou qui y a son domicile peut présenter une demande d'examen préliminaire international.

CONFIRMATION DES DESIGNATIONS FAITES PAR MESURE DE PRECAUTION

Seules les désignations expresses faites dans la requête conformément à la règle 4.9.a) figurent dans la présente notification. Il est important de vérifier si ces désignations ont été faites correctement. Des erreurs dans les désignations peuvent être corrigées lorsque des désignations ont été faites par mesure de précaution en vertu de la règle 4.9.b). Toute désignation ainsi faite peut être confirmée conformément aux dispositions de la règle 4.9.c) avant l'expiration d'un délai de 15 mois à compter de la date de priorité. En l'absence de confirmation, une désignation faite par mesure de précaution sera considérée comme retirée par le déposant. Il ne sera adressé aucun rappel ni invitation. Pour confirmer une désignation, il faut déposer une déclaration précisant l'Etat désigné concerné (avec l'indication de la forme de protection ou de traitement souhaitée) et payer les taxes de désignation et de confirmation. La confirmation doit parvenir à l'office récepteur dans le délai de 15 mois.

EXIGENCES RELATIVES AUX DOCUMENTS DE PRIORITE

Pour les déposants qui n'ont pas encore satisfait aux exigences relatives aux documents de priorité, il est rappelé ce qui suit.

Lorsque la priorité d'une demande nationale, régionale ou internationale antérieure est revendiquée, le déposant doit présenter une copie de cette demande antérieure, certifiée conforme par l'administration auprès de laquelle elle a été déposée ("document de priorité"), à l'office récepteur (qui la transmettra au Bureau international) ou directement au Bureau international, avant l'expiration d'un délai de 16 mois à compter de la date de priorité, étant entendu que tout document de priorité peut être présenté au Bureau international avant la date de publication de la demande internationale, auquel cas ce document sera réputé avoir été reçu par le Bureau international le dernier jour du délai de 16 mois (règle 17.1.a)).

Lorsque le document de priorité est délivré par l'office récepteur, le déposant peut, au lieu de présenter ce document, demander à l'office récepteur de le préparer et de le transmettre au Bureau international. La requête à cet effet doit être formulée avant l'expiration du délai de 16 mois et peut être soumise au paiement d'une taxe (règle 17.1.b)).

Si le document de priorité en question n'est pas fourni au Bureau international, ou si la demande adressée à l'office récepteur de préparer et de transmettre le document de priorité n'a pas été faite (et la taxe correspondante acquittée, le cas échéant) avant l'expiration du délai applicable mentionné aux paragraphes précédents, tout Etat désigné peut ne pas tenir compte de la revendication de priorité; toutefois, aucun office désigné ne peut décider de ne pas tenir compte de la revendication de priorité avant d'avoir donné au déposant la possibilité de remettre le document de priorité dans un délai raisonnable en l'espèce.

Lorsque plusieurs priorités sont revendiquées, la date de priorité à prendre en considération aux fins du calcul du délai de 16 mois est la date du dépôt de la demande la plus ancienne dont la priorité est revendiquée.

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire PCT 3879/BC	POUR SUITE A DONNER voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 01/ 01359	Date du dépôt international (jour/mois/année) 04/05/2001	(Date de priorité (la plus ancienne) (jour/mois/année) 09/05/2000
Déposant BULL CP8		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

☒ Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. Base du rapport

- a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

☐ la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

- b. En ce qui concerne les **séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

☐ contenu dans la demande internationale, sous forme écrite.

☐ déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

☐ remis ultérieurement à l'administration, sous forme écrite.

☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

☐ La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

☐ La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. ☐ Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (voir le cadre I).

3. ☐ Il y a absence d'unité de l'invention (voir le cadre II).

4. En ce qui concerne le **titre**,

☒ le texte est approuvé tel qu'il a été remis par le déposant.

☐ Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne l'**abrégé**,

☒ le texte est approuvé tel qu'il a été remis par le déposant

☐ le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n°

☒ suggérée par le déposant.

☐ parce que le déposant n'a pas suggéré de figure.

☐ parce que cette figure caractérise mieux l'invention.

3

☐ Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 01/01359

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F7/12

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 G07F G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	EP 0 281 058 A (SIEMENS) 7 septembre 1988 (1988-09-07) le document en entier ---	1, 2, 6-9, 12, 14
Y	FR 2 757 979 A (GEMPLUS) 3 juillet 1998 (1998-07-03) abrégé; revendications; figures ---	1, 2, 6-9, 12, 14
A	EP 0 926 624 A (OKI ELECTRIC INDUSTRY) 30 juin 1999 (1999-06-30) ---	
A	EP 0 475 837 A (GEMPLUS CARD INTERNATIONAL) 18 mars 1992 (1992-03-18) ---	
A	EP 0 531 194 A (GEMPLUS CARD INTERNATIONAL) 10 mars 1993 (1993-03-10) ---	
	-/--	



Voir la suite du cadre C pour la fin de la liste des documents



Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

- *A* document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- *E* document antérieur, mais publié à la date de dépôt international ou après cette date
- *L* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- *O* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- *P* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

- *T* document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
- *X* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- *Y* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
- *&* document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

20 juillet 2001

Date d'expédition du présent rapport de recherche internationale

30/07/2001

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

David, J

RAPPORT DE RECHERCHE INTERNATIONALE

Recherche Internationale No
PCT/FR 01/01359

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 98 37663 A (POSTGIROT BANK) 27 août 1998 (1998-08-27) -----	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 01/01359

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
EP 0281058	A	07-09-1988	AT 85444 T	15-02-1993
			DE 3877984 A	18-03-1993
			ES 2041712 T	01-12-1993
			JP 63229541 A	26-09-1988
			US 4786790 A	22-11-1988
FR 2757979	A	03-07-1998	AU 723007 B	17-08-2000
			AU 5767898 A	31-07-1998
			EP 0974131 A	26-01-2000
			WO 9829843 A	09-07-1998
EP 0926624	A	30-06-1999	JP 11191149 A	13-07-1999
EP 0475837	A	18-03-1992	FR 2666671 A	13-03-1992
			CA 2051365 A,C	13-03-1992
			DE 69100256 D	16-09-1993
			DE 69100256 T	17-02-1994
			JP 4257031 A	11-09-1992
			JP 7056629 B	14-06-1995
			US 5191608 A	02-03-1993
EP 0531194	A	10-03-1993	FR 2680892 A	05-03-1993
			JP 5217033 A	27-08-1993
			US 5343530 A	30-08-1994
WO 9837663	A	27-08-1998	SE 508844 C	09-11-1998
			AU 725952 B	26-10-2000
			AU 6126898 A	09-09-1998
			BR 9807372 A	14-03-2000
			CN 1248367 T	22-03-2000
			EP 0962071 A	08-12-1999
			NO 993939 A	19-10-1999
			SE 9700587 A	20-08-1998

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

Expéditeur : le BUREAU INTERNATIONAL

**NOTIFICATION RELATIVE
A LA PRESENTATION OU A LA TRANSMISSION
DU DOCUMENT DE PRIORITE**

(instruction administrative 411 du PCT)

Destinataire:

CORLU, Bernard
Bull CP8
PC62A24
68, route de Versailles
Boîte postale 45
F-78431 Louveciennes Cedex
FRANCE

Date d'expédition (jour/mois/année) 18 juin 2001 (18.06.01)	NOTIFICATION IMPORTANTE
Référence du dossier du déposant ou du mandataire PCT 3879/BC	
Demande internationale no PCT/FR01/01359	Date du dépôt international (jour/mois/année) 04 mai 2001 (04.05.01)
Date de publication internationale (jour/mois/année) Pas encore publiée	Date de priorité (jour/mois/année) 09 mai 2000 (09.05.00)
Déposant BULL CP8 etc	

1. La date de réception (sauf lorsque les lettres "NR" figurent dans la colonne de droite) par le Bureau international du ou des documents de priorité correspondant à la ou aux demandes énumérées ci-après est notifiée au déposant. Sauf indication contraire consistant en un astérisque figurant à côté d'une date de réception, ou les lettres "NR", dans la colonne de droite, le document de priorité en question a été présenté ou transmis au Bureau international d'une manière conforme à la règle 17.1.a) ou b).
2. Ce formulaire met à jour et remplace toute notification relative à la présentation ou à la transmission du document de priorité qui a été envoyée précédemment.
3. Un **astérisque(*)** figurant à côté d'une date de réception dans la colonne de droite signale un document de priorité présenté ou transmis au Bureau international mais de manière non conforme à la règle 17.1.a) ou b). Dans ce cas, **l'attention du déposant est appelée** sur la règle 17.1.c) qui stipule qu'aucun office désigné ne peut décider de ne pas tenir compte de la revendication de priorité avant d'avoir donné au déposant la possibilité de remettre le document de priorité dans un délai raisonnable en l'espèce.
4. Les **lettres "NR"** figurant dans la colonne de droite signalent un document de priorité que le Bureau international n'a pas reçu ou que le déposant n'a pas demandé à l'office récepteur de préparer et de transmettre au Bureau international, conformément à la règle 17.1.a) ou b), respectivement. Dans ce cas, **l'attention du déposant est appelée** sur la règle 17.1.c) qui stipule qu'aucun office désigné ne peut décider de ne pas tenir compte de la revendication de priorité avant d'avoir donné au déposant la possibilité de remettre le document de priorité dans un délai raisonnable en l'espèce.

<u>Date de priorité</u>	<u>Demande de priorité n°</u>	<u>Pays, office régional ou office récepteur selon le PCT</u>	<u>Date de réception du document de priorité</u>
09 mai 2000 (09.05.00)	00/05894	FR	05 juin 2001 (05.06.01)

<p align="center">Bureau international de l'OMPI 34, chemin des Colombettes 1211 Genève 20, Suisse</p> <p>no de télécopieur (41-22) 740.14.35</p>	<p>Fonctionnaire autorisé:</p> <p align="center">Philippe Bécamel</p> <p>no de téléphone (41-22) 338.83.38</p>
--	--

PCT

REQUÊTE

Le soussigné requiert que la présente demande internationale soit traitée conformément au Traité de coopération en matière de brevets.

Réservé à l'office récepteur

Demande internationale n°

Date du dépôt international

Nom de l'office récepteur et "Demande internationale PCT"

 Référence du dossier du déposant ou du mandataire (facultatif)
 (12 caractères au maximum)

PCT 3879/BC

Cadre n° I TITRE DE L'INVENTION Procédé pour authentifier un objet portatif, objet portatif correspondant, et appareil pour mettre en œuvre le procédé.

Cadre n° II DÉPOSANT

Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'Etat où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)

BULL CP8
68, route de Versailles
BP 45
78431 LOUVECIENNES CEDEX
FRANCE

☐ Cette personne est aussi inventeur.

n° de téléphone

(33) 1 39.66.61.76

n° de télécopieur

(33) 1 39.66.43.36

n° de téléimprimeur

Nationalité (nom de l'Etat) :

FRANCE

Domicile (nom de l'Etat) :

FRANCE

 Cette personne est
 déposant pour :

☐
tous les États
désignés
☒
tous les États désignés sauf
les États-Unis d'Amérique
☐
les États-Unis d'Amérique
seulement
☐
les États indiqués dans
le cadre supplémentaire

Cadre n° III AUTRE(S) DÉPOSANT(S) OU (AUTRE(S)) INVENTEUR(S)

Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays. Le pays de l'adresse indiquée dans ce cadre est l'Etat où le déposant a son domicile si aucun domicile n'est indiqué ci-dessous.)

HAZARD Michel
27 Rue des Harias
78124 MAREIL SUR MAULDRE
FRANCE

Cette personne est :

☐ déposant seulement

☒ déposant et inventeur

☐ inventeur seulement
 (Si cette case est cochée,
 ne pas remplir la suite.)

Nationalité (nom de l'Etat) :

FRANCE

Domicile (nom de l'Etat) :

FRANCE

 Cette personne est
 déposant pour :

☐
tous les États
désignés
☐
tous les États désignés sauf
les États-Unis d'Amérique
☒
les États-Unis d'Amérique
seulement
☐
les États indiqués dans
le cadre supplémentaire
☐ D'autres déposants ou inventeurs sont indiqués sur une feuille annexe.

Cadre n° IV MANDATAIRE OU REPRÉSENTANT COMMUN; OU ADRESSE POUR LA CORRESPONDANCE

La personne dont l'identité est donnée ci-dessous est/a été désignée pour agir au nom du ou des déposants auprès des autorités internationales compétentes, comme:

☒

mandataire

☐

représentant commun

Nom et adresse : (Nom de famille suivi du prénom; pour une personne morale, désignation officielle complète. L'adresse doit comprendre le code postal et le nom du pays.)

BULL CP8
CORLU Bernard
PC 62A24 / 68, route de Versailles - BP 45
F- 78431 LOUVECIENNES CEDEX (FRANCE)

n° de téléphone

(33) 1 39.66.61.76

n° de télécopieur

(33) 1 39.66.43.36

n° de téléimprimeur

☐ Adresse pour la correspondance : cocher cette case lorsque aucun mandataire ni représentant commun n'est/n'a été désigné et que l'espace ci-dessus est utilisé pour indiquer une adresse spéciale à laquelle la correspondance doit être envoyée.

Cadre n° V DÉSIGNATION D'ÉTATS

Les désignations suivantes sont faites conformément à la règle 4.9.a) (cocher les cases appropriées; une au moins doit l'être) :

Brevet régional

- ☐ AP Brevet ARIPO : GH Ghana, GM Gambie, KE Kenya, LS Lesotho, MW Malawi, MZ Mozambique, SD Soudan, SL Sierra Leone, SZ Swaziland, TZ République-Unie de Tanzanie, UG Ouganda, ZW Zimbabwe et tout autre État qui est un État contractant du Protocole de Harare et du PCT
- ☐ EA Brevet eurasien : AM Arménie, AZ Azerbaïdjan, BY Bélarus, KG Kirghizistan, KZ Kazakhstan, MD République de Moldova, RU Fédération de Russie, TJ Tadjikistan, TM Turkménistan et tout autre État qui est un État contractant de la Convention sur le brevet eurasien et du PCT
- ☒ EP Brevet européen : AT Autriche, BE Belgique, CH et LI Suisse et Liechtenstein, CY Chypre, DE Allemagne, DK Danemark, ES Espagne, FI Finlande, FR France, GB Royaume-Uni, GR Grèce, IE Irlande, IT Italie, LU Luxembourg, MC Monaco, NL Pays-Bas, PT Portugal, SE Suède et tout autre État qui est un État contractant de la Convention sur le brevet européen et du PCT
- ☐ OA Brevet OAPI : BF Burkina Faso, BJ Bénin, CF République centrafricaine, CG Congo, CI Côte d'Ivoire, CM Cameroun, GA Gabon, GN Guinée, GW Guinée-Bissau, ML Mali, MR Mauritanie, NE Niger, SN Sénégal, TD Tchad, TG Togo et tout autre État qui est un État membre de l'OAPI et un État contractant du PCT (si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée).

Brevet national (si une autre forme de protection ou de traitement est souhaitée, le préciser sur la ligne pointillée) :

- | | |
|--|---|
| <input type="checkbox"/> AE Émirats arabes unis | <input type="checkbox"/> LC Sainte-Lucie |
| <input type="checkbox"/> AG Antigua-et-Barbuda | <input type="checkbox"/> LK Sri Lanka |
| <input type="checkbox"/> AL Albanie | <input type="checkbox"/> LR Liberia |
| <input type="checkbox"/> AM Arménie | <input type="checkbox"/> LS Lesotho |
| <input type="checkbox"/> AT Autriche | <input type="checkbox"/> LT Lituanie |
| <input checked="" type="checkbox"/> AU Australie | <input type="checkbox"/> LU Luxembourg |
| <input type="checkbox"/> AZ Azerbaïdjan | <input type="checkbox"/> LV Lettonie |
| <input type="checkbox"/> BA Bosnie-Herzégovine | <input type="checkbox"/> MA Maroc |
| <input type="checkbox"/> BB Barbade | <input type="checkbox"/> MD République de Moldova |
| <input type="checkbox"/> BG Bulgarie | <input type="checkbox"/> MG Madagascar |
| <input checked="" type="checkbox"/> BR Brésil | <input type="checkbox"/> MK Ex-République yougoslave de Macédoine |
| <input type="checkbox"/> BY Bélarus | <input type="checkbox"/> MN Mongolie |
| <input type="checkbox"/> BZ Belize | <input type="checkbox"/> MW Malawi |
| <input checked="" type="checkbox"/> CA Canada | <input type="checkbox"/> MX Mexique |
| <input type="checkbox"/> CH et LI Suisse et Liechtenstein | <input type="checkbox"/> MZ Mozambique |
| <input checked="" type="checkbox"/> CN Chine | <input checked="" type="checkbox"/> NO Norvège |
| <input type="checkbox"/> CR Costa Rica | <input type="checkbox"/> NZ Nouvelle-Zélande |
| <input type="checkbox"/> CU Cuba | <input type="checkbox"/> PL Pologne |
| <input type="checkbox"/> CZ République tchèque | <input type="checkbox"/> PT Portugal |
| <input type="checkbox"/> DE Allemagne | <input type="checkbox"/> RO Roumanie |
| <input type="checkbox"/> DK Danemark | <input type="checkbox"/> RU Fédération de Russie |
| <input type="checkbox"/> DM Dominique | <input type="checkbox"/> SD Soudan |
| <input type="checkbox"/> DZ Algérie | <input type="checkbox"/> SE Suède |
| <input type="checkbox"/> EE Estonie | <input checked="" type="checkbox"/> SG Singapour |
| <input type="checkbox"/> ES Espagne | <input type="checkbox"/> SI Slovénie |
| <input type="checkbox"/> FI Finlande | <input type="checkbox"/> SK Slovaquie |
| <input type="checkbox"/> GB Royaume-Uni | <input type="checkbox"/> SL Sierra Leone |
| <input type="checkbox"/> GD Grenade | <input type="checkbox"/> TJ Tadjikistan |
| <input type="checkbox"/> GE Géorgie | <input type="checkbox"/> TM Turkménistan |
| <input type="checkbox"/> GH Ghana | <input type="checkbox"/> TR Turquie |
| <input type="checkbox"/> GM Gambie | <input type="checkbox"/> TT Trinité-et-Tobago |
| <input type="checkbox"/> HR Croatie | <input type="checkbox"/> TZ République-Unie de Tanzanie |
| <input type="checkbox"/> HU Hongrie | <input type="checkbox"/> UA Ukraine |
| <input type="checkbox"/> ID Indonésie | <input type="checkbox"/> UG Ouganda |
| <input type="checkbox"/> IL Israël | <input checked="" type="checkbox"/> US États-Unis d'Amérique |
| <input type="checkbox"/> IN Inde | <input type="checkbox"/> UZ Ouzbékistan |
| <input type="checkbox"/> IS Islande | <input type="checkbox"/> VN Viet Nam |
| <input checked="" type="checkbox"/> JP Japon | <input type="checkbox"/> YU Yougoslavie |
| <input type="checkbox"/> KE Kenya | <input type="checkbox"/> ZA Afrique du Sud |
| <input type="checkbox"/> KG Kirghizistan | <input type="checkbox"/> ZW Zimbabwe |
| <input type="checkbox"/> KP République populaire démocratique de Corée | |
| <input checked="" type="checkbox"/> KR République de Corée | |
| <input type="checkbox"/> KZ Kazakhstan | |

Case réservée pour la désignation d'États qui sont devenus parties au PCT après la publication de la présente feuille :

Déclaration concernant les désignations de précaution : outre les désignations faites ci-dessus, le déposant fait aussi conformément à la règle 4.9.b) toutes les désignations qui seraient autorisées en vertu du PCT, à l'exception de toute désignation indiquée dans le cadre supplémentaire comme étant exclue de la portée de cette déclaration. Le déposant déclare que ces désignations additionnelles sont faites sous réserve de confirmation et que toute désignation qui n'est pas confirmée avant l'expiration d'un délai de 15 mois à compter de la date de priorité doit être considérée comme retirée par le déposant à l'expiration de ce délai. (La confirmation (y compris les taxes) doit parvenir à l'office récepteur dans le délai de 15 mois.)

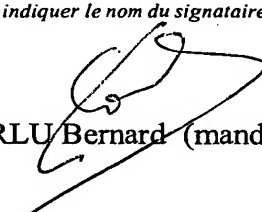
Cadre n° VI REVENDEICATION DE PRIORITÉ		<input type="checkbox"/> D'autres revendications de priorité sont indiquées dans le cadre supplémentaire.		
Date de dépôt de la demande antérieure (jour/mois/année)	Numéro de la demande antérieure	Lorsque la demande antérieure est une :		
		demande nationale : pays	demande régionale : * office régional	demande internationale : office récepteur
(1) 09 mai 2000 (09.05.2000)	000 5894	FRANCE		
(2)				
(3)				

☒ L'office récepteur est prié de préparer et de transmettre au Bureau international une copie certifiée conforme de la ou des demandes antérieures (seulement si la demande antérieure a été déposée auprès de l'office qui, aux fins de la présente demande internationale, est l'office récepteur) indiquées ci-dessus au(x) point(s) : 1

* Si la demande antérieure est une demande ARIPO, il est obligatoire d'indiquer dans le cadre supplémentaire au moins un pays partie à la Convention de Paris pour la protection de la propriété industrielle pour lequel cette demande antérieure a été déposée (règle 4.10.b)ii). Voir le cadre supplémentaire.

Cadre n° VII ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE			
Choix de l'administration chargée de la recherche internationale (ISA) (si plusieurs administrations chargées de la recherche internationale sont compétentes pour procéder à la recherche internationale, indiquer l'administration choisie; le code à deux lettres peut être utilisé) : ISA /		Demande d'utilisation des résultats d'une recherche antérieure; mention de cette recherche (si une recherche antérieure a été effectuée par l'administration chargée de la recherche internationale ou demandée à cette dernière) : Date (jour/mois/année) : 09.03.2000 Numéro : 000 5894 Pays (ou office régional) : FR FA 586 212	

Cadre n° VIII BORDEREAU; LANGUE DE DÉPÔT	
La présente demande internationale contient le nombre de feuilles suivant : requête : 03 description (sauf partie réservée au listage des séquences) : 15 revendications : 03 abrégé : 01 dessins : 02 partie de la description réservée au listage des séquences : Nombre total de feuilles : 24	Le ou les éléments cochés ci-après sont joints à la présente demande internationale : 1. <input type="checkbox"/> feuille de calcul des taxes 2. <input checked="" type="checkbox"/> pouvoir distinct signé 1 3. <input checked="" type="checkbox"/> copie du pouvoir général; numéro de référence, le cas échéant : GPA 01/0075 4. <input type="checkbox"/> explication de l'absence d'une signature 5. <input checked="" type="checkbox"/> document(s) de priorité indiqué(s) dans le cadre n° VI au(x) point(s) : 1 6. <input type="checkbox"/> traduction de la demande internationale en (langue) : 7. <input type="checkbox"/> indications séparées concernant des micro-organismes ou autre matériel biologique déposés 8. <input type="checkbox"/> listage des séquences de nucléotides ou d'acides aminés sous forme déchiffrable par ordinateur 9. <input checked="" type="checkbox"/> autres éléments (préciser) : Rapport de Recherche 586 212
Figure des dessins qui doit accompagner l'abrégé : 3	Langue de dépôt de la demande internationale : FRANCAIS

Cadre n° IX SIGNATURE DU DÉPOSANT OU DU MANDATAIRE	
À côté de chaque signature, indiquer le nom du signataire et, si cela n'apparaît pas clairement à la lecture de la requête, à quel titre l'intéressé signe. <div style="text-align: center;">  CORLU Bernard (mandataire) </div>	

Réservé à l'office récepteur	
1. Date effective de réception des pièces supposées constituer la demande internationale :	2. Dessins : <input type="checkbox"/> reçus : <input type="checkbox"/> non reçus :
3. Date effective de réception, rectifiée en raison de la réception ultérieure, mais dans les délais, de documents ou de dessins complétant ce qui est supposé constituer la demande internationale :	
4. Date de réception, dans les délais, des corrections demandées selon l'article 11.2) du PCT :	
5. Administration chargée de la recherche internationale (si plusieurs sont compétentes) : ISA /	6. <input type="checkbox"/> Transmission de la copie de recherche différée jusqu'au paiement de la taxe de recherche.

Réservé au Bureau international	
Date de réception de l'exemplaire original par le Bureau international :	

Formulaire PCT/RO/101 (dernière feuille) (juillet 1998; réimpression juillet 2000) Voir les notes relatives au formulaire de requête

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No

PCT/FR 01/01359

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

CIB 7 G07F7/12

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 7 G07F G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	EP 0 281 058 A (SIEMENS) 7 septembre 1988 (1988-09-07) le document en entier ---	1,2,6-9, 12,14
Y	FR 2 757 979 A (GEMPLUS) 3 juillet 1998 (1998-07-03) abrégé; revendications; figures ---	1,2,6-9, 12,14
A	EP 0 926 624 A (OKI ELECTRIC INDUSTRY) 30 juin 1999 (1999-06-30) ---	
A	EP 0 475 837 A (GEMPLUS CARD INTERNATIONAL) 18 mars 1992 (1992-03-18) ---	
A	EP 0 531 194 A (GEMPLUS CARD INTERNATIONAL) 10 mars 1993 (1993-03-10) ---	
	-/--	

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

- *A* document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- *E* document antérieur, mais publié à la date de dépôt international ou après cette date
- *L* document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- *O* document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- *P* document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

- *T* document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
- *X* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
- *Y* document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
- *G* document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

20 juillet 2001

Date d'expédition du présent rapport de recherche internationale

30/07/2001

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

David, J

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 98 37663 A (POSTGIROT BANK) 27 août 1998 (1998-08-27) -----	

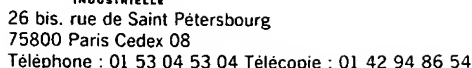
RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No

PCT/FR 01/01359

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 0281058 A	07-09-1988	AT 85444 T DE 3877984 A ES 2041712 T JP 63229541 A US 4786790 A	15-02-1993 18-03-1993 01-12-1993 26-09-1988 22-11-1988
FR 2757979 A	03-07-1998	AU 723007 B AU 5767898 A EP 0974131 A WO 9829843 A	17-08-2000 31-07-1998 26-01-2000 09-07-1998
EP 0926624 A	30-06-1999	JP 11191149 A	13-07-1999
EP 0475837 A	18-03-1992	FR 2666671 A CA 2051365 A,C DE 69100256 D DE 69100256 T JP 4257031 A JP 7056629 B US 5191608 A	13-03-1992 13-03-1992 16-09-1993 17-02-1994 11-09-1992 14-06-1995 02-03-1993
EP 0531194 A	10-03-1993	FR 2680892 A JP 5217033 A US 5343530 A	05-03-1993 27-08-1993 30-08-1994
WO 9837663 A	27-08-1998	SE 508844 C AU 725952 B AU 6126898 A BR 9807372 A CN 1248367 T EP 0962071 A NO 993939 A SE 9700587 A	09-11-1998 26-10-2000 09-09-1998 14-03-2000 22-03-2000 08-12-1999 19-10-1999 20-08-1998



Code de la propriété intellectuelle - Livre VI



REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 W 260899

REMISE DES PIÈCES DATE LIEU		Réservé à l'INPI		Cet imprimé est à remplir lisiblement à l'encre noire		DB 540 W 26089	
9 MAI 2000 75 INPI PARIS B		N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI		0005894		1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE BULL S.A. CORLU Bernard - PC/58D20 68, route de Versailles 78434 LOUVECIENNES Cedex	
Vos références pour ce dossier (facultatif)		FR 3879/BC					
Confirmation d'un dépôt par télécopie				<input type="checkbox"/> N° attribué par l'INPI à la télécopie			
2 NATURE DE LA DEMANDE		Cochez l'une des 4 cases suivantes					
Demande de brevet		<input checked="" type="checkbox"/>					
Demande de certificat d'utilité		<input type="checkbox"/>					
Demande divisionnaire		<input type="checkbox"/>					
Demande de brevet initiale		N°		Date		/ /	
ou demande de certificat d'utilité initiale		N°		Date		/ /	
Transformation d'une demande de brevet européen		<input type="checkbox"/>		N°		Date / /	
Demande de brevet initiale		N°		Date		/ /	
3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)							
PROCÉDE POUR AUTHENTIFIER UN OBJET PORTATIF, OBJET PORTATIF CORRESPONDANT, ET APPAREIL POUR METTRE EN ŒUVRE LE PROCÉDE							
4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation		Date		N°	
		Pays ou organisation		Date		N°	
		Pays ou organisation		Date		N°	
		<input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»					
5 DEMANDEUR		<input type="checkbox"/> S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»					
Nom ou dénomination sociale		BULL CP8					
Prénoms							
Forme juridique		Société Anonyme					
N° SIREN		3 2 9 5 5 6 1 4 6					
Code APE-NAF		B 3 2 1					
Adresse		Rue		BP 45 - 68, route de Versailles			
		Code postal et ville		78430 LOUVECIENNES			
Pays		France					
Nationalité		Française					
N° de téléphone (facultatif)		01.39.66.61.76					
N° de télécopie (facultatif)		01.39.66.61.73					
Adresse électronique (facultatif)		BERNARD.CORLU@BULL.NET					

REMISE DES PIÈCES DATE 9 MAI 2000 LIEU 75 INPI PARIS B N° D'ENREGISTREMENT 0005894 NATIONAL ATTRIBUÉ PAR L'INPI		Réservé à l'INPI	DB 540 W / 260899
Vos références pour ce dossier : <i>(facultatif)</i>		FR 3879/BC	
6 MANDATAIRE			
Nom		CORLU	
Prénom		Bernard	
Cabinet ou Société		BULL S.A.	
N° de pouvoir permanent et/ou de lien contractuel		PG 4280	
Adresse	Rue	68, route de Versailles / PC 58D20	
	Code postal et ville	78434 LOUVECIENNES CEDEX	
N° de téléphone <i>(facultatif)</i>		01.39.66.61.76	
N° de télécopie <i>(facultatif)</i>		01.39.66.61.73	
Adresse électronique <i>(facultatif)</i>		BERNARD.CORLU@BULL.NET	
7 INVENTEUR (S)			
Les inventeurs sont les demandeurs		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non Dans ce cas fournir une désignation d'inventeur(s) séparée	
8 RAPPORT DE RECHERCHE		Uniquement pour une demande de brevet (y compris division et transformation)	
Établissement immédiat ou établissement différé		<input checked="" type="checkbox"/> <input type="checkbox"/>	
Paiement échelonné de la redevance		Paiement en trois versements, uniquement pour les personnes physiques <input type="checkbox"/> Oui <input type="checkbox"/> Non	
9 RÉDUCTION DU TAUX DES REDEVANCES		Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention <i>(joindre un avis de non-imposition)</i> <input type="checkbox"/> Requête antérieurement à ce dépôt <i>(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence):</i>	
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		0	
10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire) CORLU Bernard (Mandataire)		VISA DE LA PRÉFECTURE OU DE L'INPI CONTRE 	

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08

Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° **1 / 1**

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

08 113 W / 260899

Vos références pour ce dossier (facultatif)		FR 3879/BC	
N° D'ENREGISTREMENT NATIONAL			
TITRE DE L'INVENTION (200 caractères ou espaces maximum) PROCEDE POUR AUTHENTIFIER UN OBJET PORTATIF, OBJET PORTATIF CORRESPONDANT, ET APPAREIL POUR METTRE EN OEUVRE LE PROCEDE ".			
LE(S) DEMANDEUR(S) : BULL CP8 BP 45 - 68, route de Versailles 78430 LOUVECIENNES - FRANCE			
DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).			
Nom		Hazard	
Prénoms		Michel	
Adresse	Rue	27 rue des Harias	
	Code postal et ville	78124	MAREIL SUR MAULDRE - FRANCE
Société d'appartenance (facultatif)			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
Nom			
Prénoms			
Adresse	Rue		
	Code postal et ville		
Société d'appartenance (facultatif)			
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)		<p>Louveciennes, le 9 mai 2000</p> <p>CORLU Bernard (Mandataire)</p>	

PROCEDE POUR AUTHENTIFIER UN OBJET PORTATIF, OBJET
PORTATIF CORRESPONDANT, ET APPAREIL POUR METTRE EN
OEUVRE LE PROCEDE

5 De nombreux domaines d'activité ont aujourd'hui recours à des objets
portatifs comportant des moyens de traitement d'information et des moyens
de mémorisation d'information, notamment sous la forme de cartes à
microprocesseur, pour sécuriser les accès aux services qu'ils offrent. Bien
que présentant un niveau de sécurité élevé, ces objets portatifs ne
10 procurent pas une sécurité totale : pour les applications les plus sensibles
(porte-monnaie électronique, carte de débit/crédit pour le paiement,
télévision à péage), l'authentification de l'objet portatif au moyen de la
cryptographie symétrique voire asymétrique s'avère insuffisante. En effet,
ce moyen d'authentification repose sur la détention, par les objets portatifs,
15 de clés secrètes. Or, l'expérience prouve que des fraudeurs, très
compétents et disposant de moyens importants, arrivent à découvrir des
clés secrètes se trouvant pourtant dans des zones mémoire normalement
inaccessibles depuis l'extérieur des objets portatifs. Une clé secrète
corrompue permet à un fraudeur ou à une organisation frauduleuse de tirer
20 un avantage substantiel en vendant à bas prix des objets portatifs clonés
offrant les mêmes services que les objets portatifs authentiques. Le
fraudeur réalisera un objet portatif clone de l'objet portatif authentique en
réalisant un produit répondant aux fonctions de l'objet portatif authentique,
sans prendre en compte tout ce qui limite l'usage de l'objet portatif et tout
25 ce qui concerne la sécurité du produit.

Dans le domaine des cartes à puce, lorsqu'un opérateur de
télécommunications, de télévision, ou une institution bancaire a recours à la
carte, il met en place une procédure d'acceptation du produit, qui comporte
deux volets :

30 1) l'homologation fonctionnelle du produit, qui garantit la conformité au
cahier des charges ;

2) l'évaluation sécuritaire du produit, qui permet de vérifier que les exigences sécuritaires sont satisfaites.

Une fois le produit accepté (sur le plan matériel et logiciel), il n'existe pas de moyen de vérifier qu'une carte a fait l'objet d'une procédure
5 d'acceptation, autre que par l'authentification utilisant une clé secrète, ce qui suppose que cette clé n'a en aucun cas pu être corrompue et ne peut donc qu'être associée à un produit accepté.

L'objet de la présente invention consiste à offrir une solution au problème posé. L'idée de base repose sur le fait qu'une clé secrète ne doit
10 pas être dissociée du produit qui l'exploite, et notamment du code ou programme exécuté par les moyens de traitement d'information de l'objet portatif. Par voie de conséquence, il convient, de façon dynamique, d'authentifier le code avant de faire confiance aux clés. Par
« authentification dynamique », on entend une authentification effectuée de
15 façon répétée au cours de la vie de l'objet portatif, plus précisément à l'occasion des différentes sessions dans lesquelles l'objet portatif est utilisé. Par exemple, dans le domaine de la télévision à péage, on authentifiera le code pendant l'émission, à intervalles de temps prédéterminés ; dans le domaine du paiement, on authentifiera le code lors de chaque transaction
20 effectuée dans le cas où le terminal coopérant avec l'objet portatif est en mode « connecté » à une autorité.

L'invention concerne à cet effet un procédé pour authentifier un objet portatif comprenant des moyens de traitement d'information et des moyens de mémorisation d'information, les moyens de mémorisation d'information
25 contenant au moins un code définissant des opérations susceptibles d'être exécutées par l'objet portatif, ainsi qu'une fonction à sens unique, caractérisé en ce qu'il comprend l'étape consistant à envoyer à l'objet portatif un ordre pour que celui-ci exécute un calcul d'un résultat en appliquant à ladite fonction à sens unique au moins une partie dudit code, ce résultat étant
30 utilisé pour décider si l'objet portatif est authentique ou non.

L'invention concerne aussi un procédé pour faire exécuter par un objet portatif une opération sensible, l'objet portatif comprenant des moyens de traitement d'information et des moyens de mémorisation d'information, les moyens de mémorisation d'information contenant au moins un code définissant des opérations susceptibles d'être exécutées par l'objet portatif, ainsi qu'une fonction à sens unique, caractérisé en ce qu'il comprend l'étape consistant à envoyer à l'objet portatif un ordre pour que celui-ci exécute un calcul d'un résultat en appliquant à ladite fonction à sens unique au moins une partie dudit code, ledit résultat intervenant dans la mise en œuvre de ladite opération sensible, cette opération n'étant réalisée avec succès que dans le cas où l'objet portatif est authentique.

L'invention concerne encore un objet portatif comprenant des moyens de traitement d'information et des moyens de mémorisation d'information, les moyens de mémorisation d'information contenant au moins un code définissant des opérations susceptibles d'être exécutées par l'objet portatif, ainsi qu'une fonction à sens unique, caractérisé en ce qu'il comprend des moyens pour exécuter un calcul d'un résultat en appliquant à ladite fonction à sens unique au moins une partie dudit code.

L'invention concerne enfin un appareil comprenant des moyens de traitement d'information et des moyens de mémorisation d'information et agencé pour communiquer avec un objet portatif afin d'authentifier celui-ci, l'objet portatif comprenant des moyens de traitement d'information et des moyens de mémorisation d'information, les moyens de mémorisation d'information de l'objet portatif contenant au moins un code définissant des opérations susceptibles d'être exécutées par l'objet portatif, ainsi qu'une fonction à sens unique, caractérisé en ce qu'il comprend des moyens pour envoyer à l'objet portatif un ordre pour que celui-ci exécute un calcul d'un résultat en appliquant à ladite fonction à sens unique au moins une partie dudit code de l'objet portatif.

D'autres détails et avantages de la présente invention apparaîtront au cours de la description suivante d'un mode d'exécution préféré mais non limitatif, en regard des dessins annexés sur lesquels :

5 La figure 1 représente un objet portatif coopérant avec un dispositif de traitement d'information ;

 La figure 2 est un organigramme d'une procédure de vérification d'une signature calculée par un objet portatif sur un code qu'il détient ;

 La figure 3 représente un format de message envoyé à l'objet portatif
10 pour que celui-ci calcule une signature de code ; et

 La figure 4 représente une procédure d'authentification d'une carte à puce, conformément aux normes GSM.

 La figure 1 représente un dispositif de traitement d'information 1
15 coopérant avec un objet portatif 7. Le dispositif de traitement d'information comprend de façon connue en soi des moyens de traitement d'information 2 auxquels sont reliés une mémoire non volatile 3, une mémoire RAM 4, des moyens 5 pour coopérer, avec ou sans contact physique, avec l'objet portatif 7, et une interface de transmission 6 permettant au dispositif de traitement
20 d'information de communiquer avec un réseau de communication d'information. Le dispositif de traitement d'information 1 peut en outre être équipé de moyens de stockage tels que des disquettes ou disques amovibles ou non, de moyens de saisie (tels qu'un clavier et/ou un dispositif de pointage du type souris) et de moyens d'affichage, ces différents moyens
25 n'étant pas représentés sur la figure 1.

 Le dispositif de traitement d'information peut être constitué par tout appareil informatique installé sur un site privé ou public et apte à fournir des moyens de gestion de l'information ou de délivrance de divers biens ou services, cet appareil étant installé à demeure ou portable. Il peut notamment
30 s'agir aussi d'un appareil dédié aux télécommunications.

Par ailleurs, l'objet portatif 7 porte une puce incluant des moyens de traitement d'information 8, reliés d'un côté à une mémoire non volatile 9 et à une mémoire volatile de travail RAM 10, et reliés d'un autre côté à des moyens 11 pour coopérer avec le dispositif de traitement d'information 1. La

5 mémoire non volatile 9 peut comprendre une partie non modifiable ROM et une partie modifiable EPROM, EEPROM, ou constituée de mémoire RAM du type "flash" ou FRAM (cette dernière étant une mémoire RAM ferromagnétique), c'est-à-dire présentant les caractéristiques d'une mémoire EEPROM avec en outre des temps d'accès identiques à ceux d'une RAM

10 classique.

En tant que puce, on pourra notamment utiliser un microprocesseur autoprogrammable à mémoire non volatile, tel que décrit dans le brevet américain n° 4.382.279 au nom de la Demanderesse. Dans une variante, le microprocesseur de la puce est remplacé - ou tout du moins complété - par

15 des circuits logiques implantés dans une puce à semi-conducteurs. En effet, de tels circuits sont aptes à effectuer des calculs, notamment d'authentification et de signature, grâce à de l'électronique câblée, et non microprogrammée. Ils peuvent notamment être de type ASIC (de l'anglais « Application Specific Integrated Circuit »). Avantageusement, la puce sera

20 conçue sous forme monolithique.

L'objet portatif stocke, dans une zone de sa mémoire non volatile 9 qui est de préférence accessible seulement aux moyens de traitement 8, un code ou programme de fonctionnement incluant l'un ou/et l'autre des programmes suivants :

- 25 -un système d'exploitation correspondant à un programme gérant des fonctions de base de l'objet portatif ;
- un programme effectuant une interprétation entre un langage système et un langage de plus haut niveau ;
- un ou plusieurs programmes d'application correspondant à une ou plusieurs
- 30 applications offertes par l'objet portatif (application carte bancaire,

application porte-monnaie électronique, application contrôle d'accès des personnes, etc...).

De préférence et comme expliqué par la suite, ce code inclura une partie de « programme machine » ou programme écrit avec un langage
5 propre aux moyens de traitement 8.

Ce code peut être stocké dans une zone de mémoire ROM masquée ou dans une zone de mémoire EEPROM de la mémoire non volatile 9, ou encore en partie dans ces deux zones. Le code inclut une routine de signature apte à calculer une signature d'une partie paramétrable du code.
10 Avantageusement, la routine de signature comprend une fonction apte à calculer un condensé de la partie de code : il s'agit par exemple d'un checksum (ou somme de contrôle) ou d'une fonction de hachage telle que MD5 ou SHA, manipulant des bits du code en leur appliquant une fonction mathématique. La routine de signature comprend encore un algorithme de
15 signature apte à signer le condensé de la partie de code : il peut s'agir d'un algorithme symétrique tel que le triple DES (de l'anglais Data Encryption Standard) en mode « MAC » (de l'anglais « Message Authentication Code » ou code d'authentification de message) ou d'un algorithme asymétrique tel que le RSA (des auteurs Rivest, Shamir, et Adleman). L'algorithme de
20 signature utilise une clé secrète K_1 qui, soit est fournie à l'objet portatif au moment de calculer la signature, soit est stockée dans une zone secrète de la mémoire non volatile 9 de l'objet portatif, accessible aux seuls moyens de traitement d'information 8. Un avantage de la première solution est qu'elle permet de modifier dans le temps la clé secrète utilisée. Dans le cas où la clé
25 secrète K_1 est fournie à l'objet portatif, elle l'est de préférence sous forme chiffrée au moyen d'une autre clé K_2 , l'objet portatif détenant, selon le type d'algorithme de chiffrement utilisé, soit cette même clé, soit une clé corrélée à celle-ci, en vue de déchiffrer la clé secrète K_1 . De façon connue en soi, le calcul de signature comme celui de chiffrement fait intervenir un aléa fourni à
30 l'objet portatif.

La procédure de communication avec l'objet portatif est représentée sur la figure 2. On suppose que le terminal doit donner à l'objet portatif un ordre d'exécuter une opération sensible déterminée, opération qui requiert au préalable l'authentification du code contenu dans l'objet portatif. A l'étape 5 21, le terminal 1 transmet à l'objet portatif un ordre de lecture d'informations d'identification de l'objet portatif, stockées en mémoire de l'objet portatif et définissant le type de la puce portée par cet objet et le numéro de version de son système d'exploitation. A l'étape 22, le terminal 1 transmet à l'objet portatif un ordre de calcul de signature pour que celui-ci exécute la routine de signature. Selon une première forme de réalisation dans laquelle le terminal est en mode « connecté » à une autorité via un réseau de communication d'information, c'est-à-dire à un organisme responsable d'une opération sensible à exécuter par l'objet portatif, l'ordre de calcul de signature est émis par l'autorité, le terminal se contentant de transmettre cet 10 ordre à l'objet portatif. Selon une seconde forme de réalisation dans laquelle le terminal est en mode « non connecté » à l'autorité, l'ordre de calcul de signature est émis par le terminal lui-même. Dans tous les cas, l'ordre de calcul de signature prend la forme d'un message dont le format est, selon une forme de réalisation préférée, représenté à la figure 3. Ce message 15 comprend tout d'abord un ordre 31 d'exécuter la routine de signature. Il comprend ensuite, pour chaque code i d'un ensemble de codes 1 à n éventuellement impliqués dans le calcul de signature, une adresse de début $32i$ désignant l'endroit du code i de l'objet portatif où doit commencer la partie de code à considérer, une adresse de fin $33i$ où doit se terminer cette 20 partie de code, et un pas $34i$ définissant, parmi les octets composant le code i , ceux qui seront considérés : par exemple, si ce pas est égal à 7, cela signifie que l'objet portatif considérera, pour son calcul, un octet sur sept, soit le premier octet, puis le huitième, puis le quinzième, etc...Le message comprend ensuite un aléa E (35) qui interviendra dans le calcul de signature puis, seulement dans le cas où la clé secrète de signature n'est pas stockée 30 dans l'objet portatif, cette clé secrète de signature K_1' (36), chiffrée. De

préférence, les valeurs suivantes changent à chaque procédure de vérification de signature : adresses de début, adresses de fin, pas, aléa E ; on notera cependant qu'une sécurité satisfaisante est déjà obtenue en ne faisant varier que l'une de ces valeurs.

5 On notera que, dans le cas où l'un des codes impliqués dans le calcul de signature est écrit en un langage évolué et non dans le langage machine propre aux moyens de traitement 8 de l'objet portatif, ce qui est peut être par exemple le cas pour une application bancaire, les adresses de début 32i et de fin 33i sont remplacées par un identifiant général de ce code.

10 De préférence, lorsque la clé secrète de signature K_1' est présente dans le message, le message inclura en outre un checksum ou une signature du message. A réception du message par l'objet portatif, celui-ci recalculera le checksum ou la signature, ce qui lui permettra :

-de s'assurer de l'origine du message ;

15 -de vérifier qu'il n'y a pas eu d'incident de transmission.

A l'étape 23, l'objet portatif exécute le calcul de signature. Dans le cas où il a reçu la clé secrète chiffrée K_1' , il déchiffre cette clé au moyen d'une clé de déchiffrement. Il calcule un condensé des parties de code à considérer, puis il signe ce condensé avec la clé secrète K_1 en faisant
20 intervenir l'aléa E. A l'étape 24, l'objet portatif transmet la signature ainsi calculée au terminal 1.

Dans le cas où le terminal fonctionne en mode « non connecté », il vérifie lui-même la signature (étape 25). De préférence, le terminal ne connaît ni le (les) code(s) authentique(s), ni la clé K_1 , laquelle est supposée
25 être détenue par l'objet portatif. L'autorité fournit au terminal un message conforme à la figure 3, à l'exception de la clé K_1' , et une signature précalculée correspondant à ce message particulier. Le terminal enverra à l'objet portatif ledit message et, à réception de la signature en provenance de l'objet portatif, vérifiera celle-ci par comparaison avec sa signature
30 précalculée. Si la comparaison aboutit positivement, le ou les codes de l'objet portatif sont authentifiés et le terminal donne l'ordre à l'objet portatif

d'exécuter l'opération sensible précitée (étape 26). Dans la négative, le terminal met au rebut ou rejette l'objet portatif (étape 27).

Dans le cas où le terminal fonctionne en mode « connecté » à une autorité, c'est l'autorité qui émet le message de la figure 3, lequel sera retransmis par le terminal à l'objet portatif. L'autorité stocke à cet effet dans
 5 une mémoire le ou les codes de l'objet portatif et, soit la clé secrète K_1 , soit une clé corrélée à celle-ci. elle stocke aussi en mémoire les autres paramètres contenus dans le message de la figure 3. L'autorité peut, soit précalculer ou recalculer la signature en utilisant l'algorithme de signature et
 10 la clé secrète K_1 et la comparer avec la signature reçue de l'objet portatif (étape 25) via le terminal, soit utiliser la signature reçue de l'objet portatif pour recalculer le condensé des codes de l'objet portatif en utilisant un algorithme inverse de l'algorithme de signature et, selon l'algorithme utilisé, soit la clé secrète K_1 , soit ladite clé corrélée à celle-ci ; l'autorité compare
 15 ensuite le condensé ainsi recalculé avec un condensé des codes qu'elle détient en mémoire. C'est aussi l'autorité qui déclenchera l'exécution de l'opération sensible (étape 26, figure 2) ou la mise au rebut ou le rejet de l'objet portatif (étape 27), le terminal servant seulement d'intermédiaire. On notera que la procédure en mode « terminal connecté à l'autorité » est plus
 20 fiable que celle en mode « terminal non connecté à l'autorité ».

En variante, la signature calculée par l'objet portatif n'est pas envoyée à l'extérieur juste après son calcul, mais est conservée dans l'objet portatif et mise à disposition du monde extérieur de façon qu'elle puisse être lue ultérieurement.

25 En cas de fraude, une clé a généralement pu être découverte par le fraudeur, permettant à celui-ci d'émettre une quantité importante d'objets portatifs clones, contenant cette clé. Ces objets portatifs contiennent un code réduit assurant seulement les fonctionnalités indispensables pour mettre en oeuvre une application que vise à utiliser le fraudeur, à l'exclusion
 30 notamment des fonctions sécuritaires : ce code est donc différent du ou des codes d'un objet portatif authentique. La procédure de la figure 2 produira

une signature non conforme à la signature authentique, ce qui permettra d'écarter tous ces objets portatifs.

Si le ou les codes des objets portatifs authentiques contiennent un code machine, l'authentification est encore plus fiable. En effet, supposons
5 que le fraudeur ait pu arriver, à l'aide de moyens très perfectionnés, à obtenir le code contenu dans un objet portatif authentique : il doit alors, pour que les objets portatifs clones puissent se faire authentifier, mettre ce code dans chaque objet portatif clone sous forme de table de données, en plus du code non authentique contenu dans les objets portatifs clones, afin que le calcul
10 d'authentification porte sur le code authentique. En effet, l'objet portatif clone utilisera le plus souvent des moyens de traitement différents de ceux de l'objet portatif authentique, c'est-à-dire utilisant un code machine écrit dans un langage différent, ce code machine ne permettant pas d'aboutir à une authentification réussie. La nécessité, pour le fraudeur, de stocker dans
15 chaque objet portatif, outre son propre code, celui d'un objet portatif authentique, constitue un handicap important qui est de nature à décourager la fraude.

Un premier exemple d'opération sensible à sécuriser est le suivant : il
20 s'agit d'une opération de personnalisation d'objets portatifs constitués par des cartes à puce. Cette opération, effectuée chez une autorité, consiste à stocker, dans une zone secrète de la mémoire non volatile des cartes, des clés « émetteur » appartenant à l'organisme émetteur des cartes considérées, ainsi que des clés « applicatives », permettant aux cartes
25 d'avoir accès à différentes applications. Selon l'invention, le stockage de ces clés en carte ne s'effectuera que si la procédure de vérification de la figure 2 aboutit positivement.

Un deuxième exemple d'opération sensible à sécuriser est celui de la télévision à péage. Ce domaine est l'objet de fraude permanente affectant un
30 appareil décodeur d'image utilisé dans cette application, et plus récemment les cartes utilisées en association avec cet appareil. Les cartes clones

contiennent un code réduit permettant de délivrer une clé de désembrouillage de l'image de télévision.

Dans un mode de fonctionnement classique, chaque carte de télévision reçoit périodiquement des messages dits « de contrôle », qui
5 contiennent des données de contrôle (date, droits, etc..., et une clé de désembrouillage chiffrée) ; l'ensemble de chaque message est signé. La carte vérifie la signature, puis déchiffre la clé de désembrouillage. Selon l'invention, on ne délivre pas à la carte la clé de désembrouillage mais un message du type de celui de la figure 3, lui demandant d'effectuer un calcul
10 sur une partie du ou des code(s) de la carte, calcul dont le résultat constitue la clé de désembrouillage si et seulement si le code de la carte est authentique. On constate donc que, dans cet exemple, la carte ne transmet pas de résultat de calcul à une autorité pour son authentification, l'authentification étant implicite et se manifestant par le désembrouillage
15 effectif de l'image de télévision.

Un troisième exemple d'opération sensible à sécuriser concerne le domaine des cartes de débit/crédit. Avant que le terminal n'autorise une opération de débit/crédit de la carte, il déclenchera la procédure de la figure 2, de préférence en mode « connecté » à une autorité bancaire.

20 Avantageusement, l'organisme émetteur des objets portatifs communiquera aux organismes utilisateurs de ces objets portatifs, comme moyen de vérification de l'authenticité de ces objets portatifs à l'occasion de leur personnalisation et avant leur diffusion à des usagers individuels, au moins un objet portatif de référence dûment authentifié par l'organisme
25 émetteur. L'authentification d'un objet portatif consistera à faire calculer une signature du code à la fois dans cet objet portatif et dans l'objet portatif de référence, la comparaison des deux résultats permettant de conclure sur l'authenticité de l'objet portatif à vérifier. La sélection, par l'organisme utilisateur, de l'objet portatif de référence approprié parmi un ensemble
30 d'objets portatifs de référence éventuellement détenus par cet organisme s'effectue au moyen des informations d'identification précitées (étape 21 de

la figure 2). Ce procédé a l'avantage, pour l'organisme émetteur des objets portatifs, de ne pas communiquer aux organismes utilisateurs le contenu du (des) code(s) des objets portatifs, c'est-à-dire son savoir-faire. Il est donc plus sécuritaire pour lui.

5 Avantageusement, la procédure de la figure 2 sera précédée d'une opération d'authentification de la personne ou de l'organisme mettant en oeuvre cette procédure, selon des moyens connus basés sur la détention, par cette personne ou cet organisme, d'un PIN (de l'anglais Personal Identification Number) ou mieux d'une clé.

10 Selon une variante de réalisation de l'invention moins avantageuse, le procédé d'authentification de l'objet portatif consiste à vérifier la signature de d'une partie fixe du code contenu dans cet objet portatif, éventuellement de l'ensemble du code, et non d'une partie de celui-ci variable lors de chaque procédure d'authentification.

15 Selon une autre variante de réalisation de l'invention moins avantageuse, le procédé d'authentification de l'objet portatif n'inclut pas l'opération consistant à condenser le code avant sa signature.

 On notera que, si le code est stocké dans l'objet portatif en laissant des espaces mémoire vides, il sera avantageux de combler ces espaces
20 avec un code fictif qui ne remplira aucune fonction mais rendra le code plus volumineux, ce qui gênera d'autant plus le fraudeur dans sa tentative de recopier ce code sur des objets portatifs clones. Par « code fictif », on entend un code écrit dans un langage réel mais qui ne sera jamais utilisé, c'est-à-dire jamais exécuté. Par opposition, le code effectivement utilisé sera appelé
25 « code réel ».

 Il existe le risque qu'un fraudeur arrive à identifier le code manipulé lors de l'opération de signature selon l'invention, en observant le bruit généré par l'objet portatif. Selon l'invention, on limite ce risque en ne signant du code réel que de temps en temps, notamment à l'occasion d'opérations
30 jugées cruciales du point de vue sécuritaire. Une telle opération est par exemple celle de personnalisation de l'objet portatif, dans laquelle des

moyens applicatifs sont insérés dans l'objet portatif, notamment des clés et des codes applicatifs. Par contre, lors d'opérations courantes moins sensibles et plus répétitives, il sera demandé à l'objet portatif de signer du code fictif.

5

Il serait utile d'empêcher un fraudeur de se faire passer pour une autorité habilitée en interrogeant l'objet portatif selon la procédure de la figure 2, et en répétant cette opération un grand nombre de fois, de façon à observer les informations circulant dans l'objet portatif. A cet effet, et selon
10 un perfectionnement de l'invention, l'objet portatif est agencé pour limiter le nombre d'appels à la routine de signature à un nombre prédéterminé.

Une application de l'invention au domaine GSM (de l'anglais « Global System for Mobile communications ») va maintenant être présentée. La
15 figure 4 rappelle le procédé défini par les normes GSM, d'authentification par un serveur d'authentification 41, de la carte à puce 42 équipant un mobile GSM 43. On rappelle que le mobile 43 dialogue avec le serveur 41 via une base station 44. Le procédé comprend une première étape selon laquelle la carte envoie au serveur un identifiant IMSI définissant l'identité d'un abonné
20 porteur du mobile, ainsi que l'identité de la carte, donc du code qui y est contenu. En réponse, le serveur envoie à la carte un aléa. A partir de cet aléa, la carte exécute une commande connue sous le nom de « RUN GSM ALGO » calculant une valeur d'authentification nommée SRES' et une clé K_c à partir d'une clé KI propre à la carte. De son côté, le serveur calcule une
25 valeur d'authentification de référence SRES'. La carte envoie ensuite sa valeur d'authentification SRES au serveur, lequel la compare à sa valeur d'authentification de référence SRES' afin de déterminer si la carte est authentique ou non.

Selon l'invention, le procédé d'authentification ci-dessus est modifié
30 comme suit : au lieu d'envoyer à la carte un aléa classique constitué par un nombre défini par le serveur, celui-ci lui envoie le message de la figure 3. A

réception, la carte calcule une signature de code selon l'étape 23 de la figure 2, basée sur une clé de signature déterminée K_1 . Ensuite, la carte calcule la valeur d'authentification SRES conformément aux normes GSM, mais en utilisant, en tant qu'aléa, le résultat de la signature de code au lieu de l'aléa habituellement fourni par le serveur. De préférence, le procédé selon l'invention ne sera pas mis en œuvre lors de chaque session entre le mobile et le serveur mais seulement de temps en temps, de façon à réduire le risque qu'un fraudeur arrive à identifier le code manipulé lors de l'opération de signature selon l'invention, en observant le bruit généré par la carte.

10 Dans ce qui précède, on a décrit une authentification du code de l'objet portatif par calcul de signature. En variante, on peut effectuer cette authentification au moyen d'un calcul de chiffrement/déchiffrement, comme cela est connu en soi. Dans le cas d'un algorithme symétrique, l'objet portatif calculera un chiffré de son code avec une clé secrète et l'enverra au terminal

15 ou à l'autorité qui effectuera l'authentification par chiffrement ou déchiffrement. Dans le cas d'un algorithme asymétrique, l'objet portatif calculera un chiffré de son code avec une clé publique et l'enverra au terminal ou à l'autorité qui effectuera l'authentification par chiffrement ou déchiffrement. Par ailleurs, on a présenté dans ce qui précède un calcul

20 d'authentification qui mettait en œuvre un algorithme cryptographique manipulant une ou plusieurs clés, dont l'une est secrète. Un tel algorithme, comme le DES ou RSA précités, est dit « trap-door one way », les termes « one way » signifiant que la fonction utilisée est à sens unique, et les termes « trap-door » signifiant qu'il existe un secret. On rappelle qu'une fonction à

25 sens unique est une fonction qui peut être calculée dans un sens sans information particulière, mais qui ne peut pas être calculée de façon inverse, sauf éventuellement si l'on connaît certains paramètres. Dans le cas du DES et du RSA, ces paramètres consistent dans la clé secrète. Selon l'invention, l'utilisation d'une fonction « trap-door » est intéressante en ce qu'elle apporte

30 une sécurité supplémentaire basée sur la clé secrète, mais elle n'est pas nécessaire : il suffit en effet, pour réaliser l'opération d'authentification du

code de l'objet portatif, d'effectuer un calcul sur ce code avec toute fonction à sens unique, en l'absence de toute manipulation de clé. Une fonction à sens unique est notamment une fonction de hachage telle que MD5 ou SHA citées précédemment.

REVENDICATIONS

1. Procédé pour authentifier un objet portatif (7) comprenant des moyens de traitement d'information (8) et des moyens de mémorisation d'information (9,10), les moyens de mémorisation d'information contenant au moins un code (i) définissant des opérations susceptibles d'être exécutées par l'objet portatif, ainsi qu'une fonction à sens unique, caractérisé en ce qu'il comprend l'étape consistant à envoyer à l'objet portatif un ordre (31,32i-34i, 35,36) pour que celui-ci exécute un calcul d'un résultat en appliquant à ladite fonction à sens unique au moins une partie dudit code (i), ce résultat étant utilisé pour décider si l'objet portatif est authentique ou non.

2. Procédé selon la revendication 1, dans lequel ledit résultat intervient dans la mise en œuvre d'une opération déterminée, cette opération n'étant réalisée avec succès que dans le cas où l'objet portatif (7) est authentique.

3. Procédé selon la revendication 2, dans lequel ladite opération déterminée comprend un déchiffrement d'information, ledit résultat permettant de produire une clé de déchiffrement associée.

4. Procédé selon la revendication 1, dans lequel ladite partie de code (i) utilisée dans le calcul comprend une partie de code machine.

5. Procédé selon la revendication 1, dans lequel l'objet portatif (7) contient un code dit « réel » définissant des opérations destinées à être exécutées par l'objet portatif, et un code dit « fictif » définissant des opérations non destinées à être exécutées par l'objet portatif, ladite partie de code utilisée dans le calcul comprenant une partie de code fictif.

6. Procédé selon la revendication 1, dans lequel ledit ordre (31,32i-34i, 35,36) est envoyé de façon répétitive à l'objet portatif au cours de sa vie, avant l'exécution, par celui-ci, desdites opérations.

5 7. Procédé selon la revendication 1, dans lequel ladite partie de code (i) utilisée dans le calcul est définie par une adresse de début (32i) et une adresse de fin (33i) dans les moyens de mémorisation d'information, lesdites adresses étant envoyées à l'objet portatif.

10 8. Procédé selon la revendication 1, dans lequel ledit code (i) comprend un ensemble de mots binaires, ladite partie de code utilisée dans le calcul étant définie par un sous-ensemble de mots binaires comprenant les mots binaires répartis dans les moyens de mémorisation d'information selon un pas déterminé (34i), ledit pas étant envoyé à l'objet portatif.

15 9. Procédé pour faire exécuter par un objet portatif (7) une opération sensible, l'objet portatif comprenant des moyens de traitement d'information (8) et des moyens de mémorisation d'information (9,10), les moyens de mémorisation d'information contenant au moins un code (i) définissant des
20 opérations susceptibles d'être exécutées par l'objet portatif, ainsi qu'une fonction à sens unique, caractérisé en ce qu'il comprend l'étape consistant à envoyer à l'objet portatif un ordre (31,32i-34i, 35,36) pour que celui-ci exécute un calcul d'un résultat en appliquant à ladite fonction à sens unique au moins une partie dudit code (i), ledit résultat intervenant dans la mise en
25 œuvre de ladite opération sensible, cette opération n'étant réalisée avec succès que dans le cas où l'objet portatif (7) est authentique.

10. Procédé selon la revendication 9, dans lequel ladite partie de code (i) utilisée dans le calcul comprend une partie de code machine.

11. Procédé selon la revendication 9, dans lequel l'objet portatif contient un code dit « réel » définissant des opérations destinées à être exécutées par l'objet portatif, et un code dit « fictif » définissant des opérations non destinées à être exécutées par l'objet portatif, ladite partie de
5 code utilisée dans le calcul comprenant une partie de code fictif.

12. Objet portatif comprenant des moyens de traitement d'information (8) et des moyens de mémorisation d'information (9,10), les moyens de mémorisation d'information contenant au moins un code (i) définissant des
10 opérations susceptibles d'être exécutées par l'objet portatif, ainsi qu'une fonction à sens unique, caractérisé en ce qu'il comprend des moyens pour exécuter un calcul d'un résultat en appliquant à ladite fonction à sens unique au moins une partie dudit code.

13. Objet portatif selon la revendication 12, dans lequel ladite partie de code (i) utilisée dans le calcul comprend une partie de code machine.

14. Appareil (1) comprenant des moyens de traitement d'information (2) et des moyens de mémorisation d'information (3,4) et agencé pour
20 communiquer avec un objet portatif (7) afin d'authentifier celui-ci, l'objet portatif comprenant des moyens de traitement d'information (8) et des moyens de mémorisation d'information (9,10), les moyens de mémorisation d'information de l'objet portatif contenant au moins un code (i) définissant des opérations susceptibles d'être exécutées par l'objet portatif, ainsi qu'une
25 fonction à sens unique, caractérisé en ce qu'il comprend des moyens pour envoyer à l'objet portatif un ordre (31,32i-34i, 35,36) pour que celui-ci exécute un calcul d'un résultat en appliquant à ladite fonction à sens unique au moins une partie dudit code (i) de l'objet portatif.

15. Appareil selon la revendication 14, dans lequel ladite partie de code (i) utilisée dans le calcul comprend une partie de code machine.

19
ABREGE

L'invention concerne un procédé pour authentifier un objet portable comprenant des moyens de traitement d'information et des moyens de
5 mémorisation d'information, les moyens de mémorisation d'information contenant au moins un code (i) définissant des opérations susceptibles d'être exécutées par l'objet portable, ainsi qu'une fonction à sens unique.

Selon l'invention, ce procédé comprend l'étape consistant à envoyer à l'objet portable un ordre (31,32i-34i, 35,36) pour que celui-ci exécute un calcul
10 d'un résultat en appliquant à ladite fonction à sens unique au moins une partie dudit code (i), ce résultat étant utilisé pour décider si l'objet portable est authentique ou non.

L'invention concerne aussi l'objet portable associé et un appareil
15 destiné à coopérer avec l'objet portable.

Figure 3

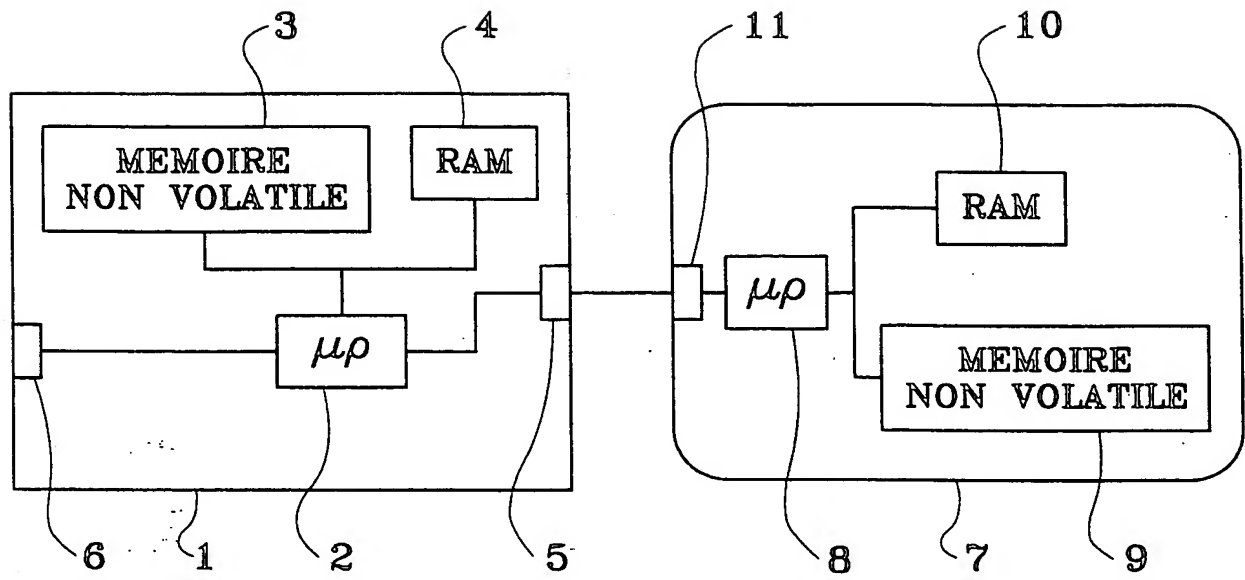


FIG. 1

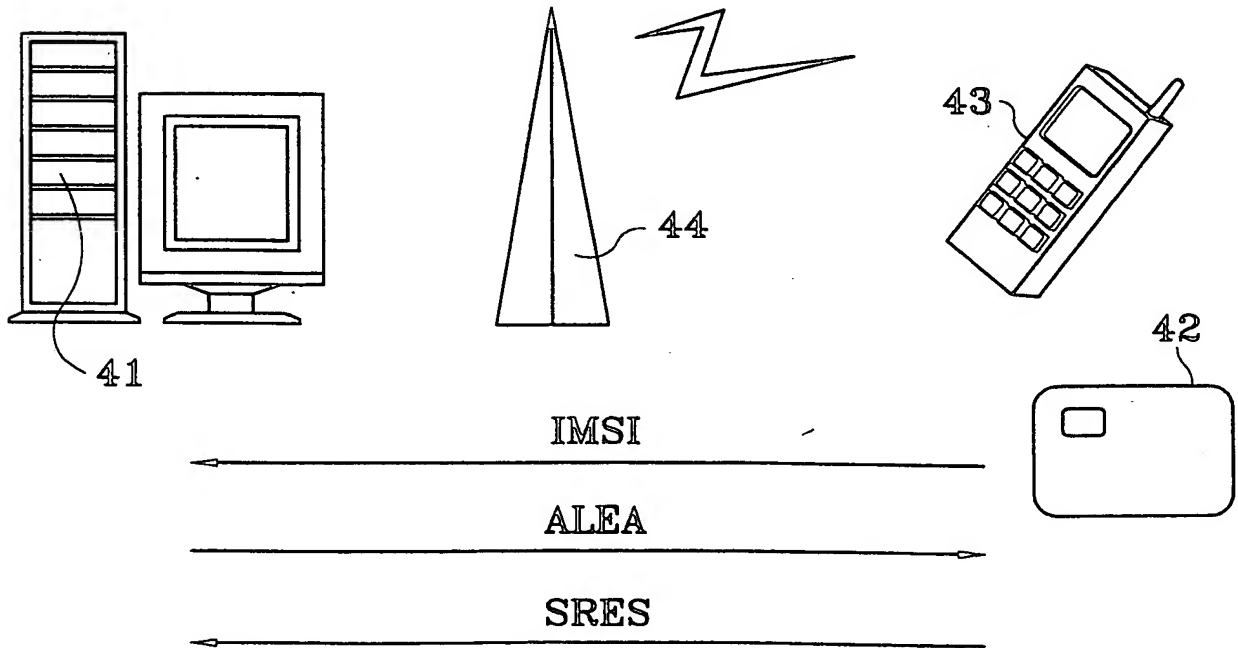


FIG. 4

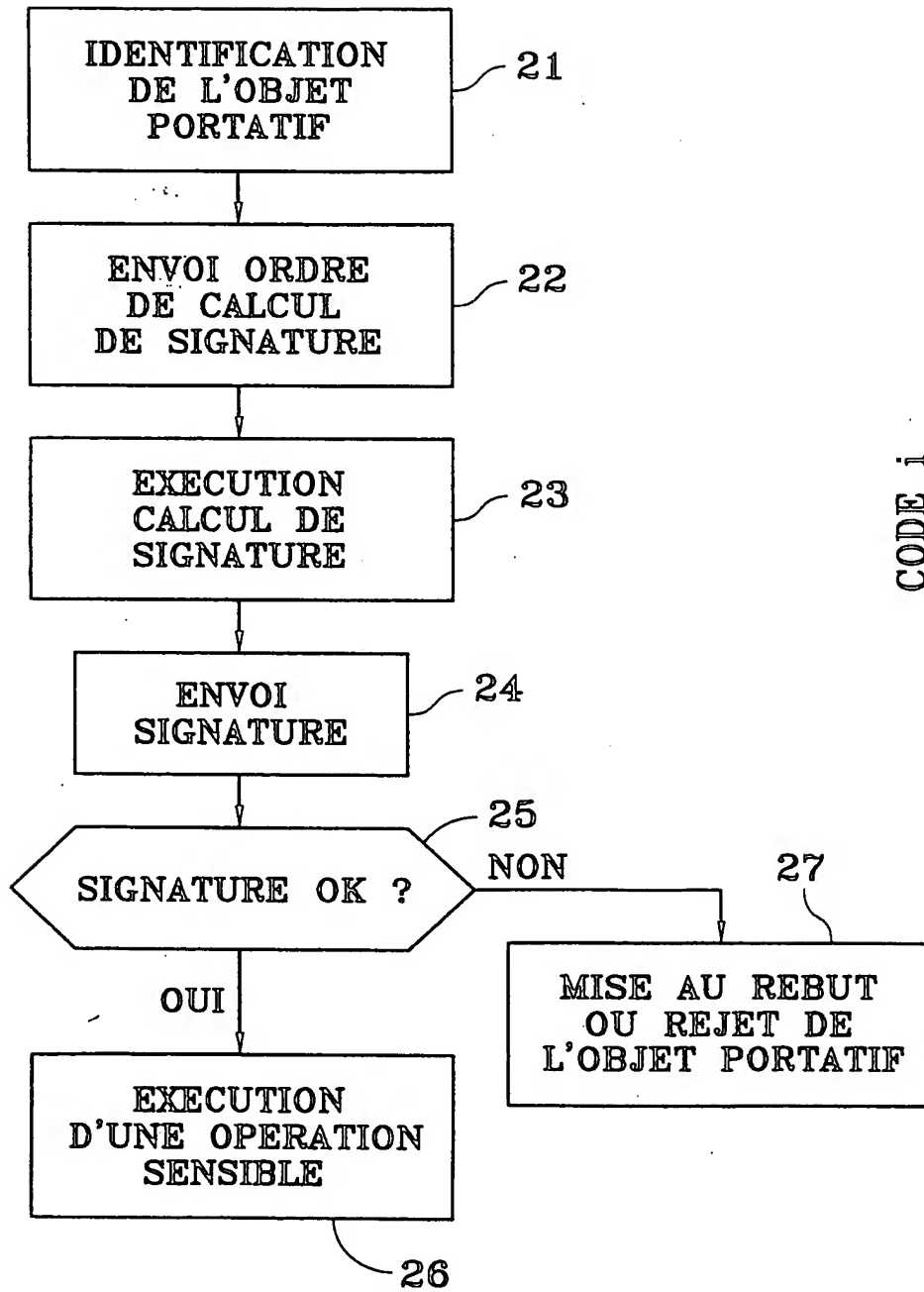


FIG.2

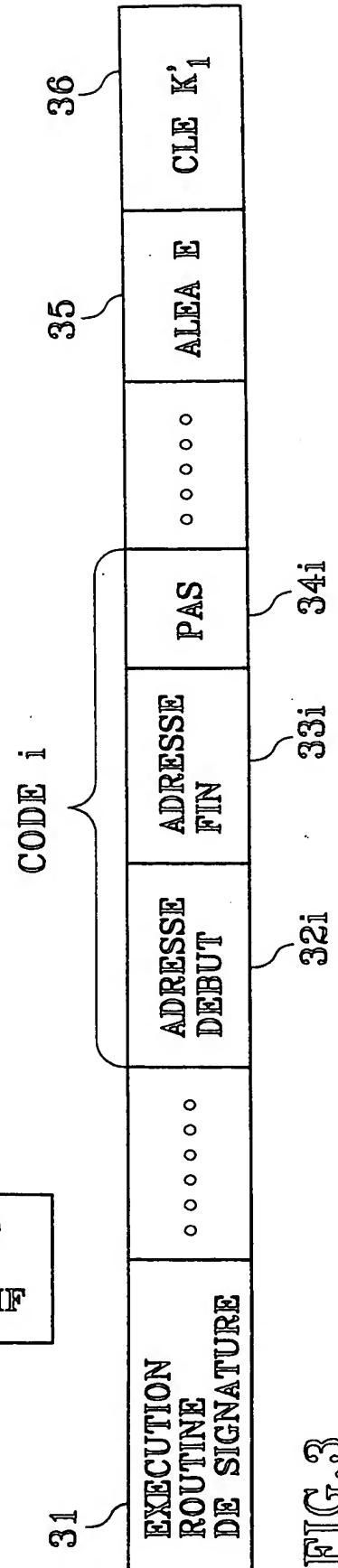


FIG.3